

BEZPIECZNA PODRÓŻ

Kradzież bagażu, pieniędzy, zgubienie rzeczy osobistych? Boli, ale z tym można sobie jakoś poradzić. Dziś największym zagrożeniem staje się kradzież informacji. Także w podróży, zarówno tej służbowej, jak i prywatnej.

Pośpiech, urlopowa beztroska czy nieznajomość języka – wszystko to sprawia, że ryzyko kradzieży informacji rośnie. Poczynając od utraty walizki, w którym akurat znajdował się przenośny komputer, poprzez wyłudzenie numeru karty kredytowej, a kończąc na lekkomyślnym podaniu danych osobowych. Straty mogą być naprawdę poważne. Na szczęście to, czy padniemy ofiarą wyłudzenia informacji zależy w znacznej mierze od nas.

Po pierwsze okazja czyni złodzieja. Kiedy w podróży posługujemy się notebookiem tak, że wszyscy dookoła mogą przeczytać informacje znajdujące się na ekranie czy głośno przez telefon omawiamy ważne kontrakty, sami prosimy się o nieszczęście. Jeżeli już musimy zostawić laptopa w hotelu, pamiętajmy o zabezpieczeniu go hasłem uniemożliwiającym uruchomienie systemu. Nawet gdy stracimy komputer, nie stracimy informacji.

Kolejna niebezpieczna sytuacja to internetowa rezerwacja biletu lotniczego czy hotelu. Po pierwsze: zawsze korzystajmy z oficjalnych stron. Przenoszenie na strony o zupełnie innym adresie powinno od razu wzbudzać w nas podejrzliwość. Podobnie jak sytuacja, w której ktoś żąda od nas weryfikacji lub podania danych osobowych przy pomocy e-maila. Pamiętajmy, żadna z szanujących się instytucji nie prowadzi weryfikacji informacji o osobach w ten sposób! Zawsze sprawdzajmy adres, z którego przychodzi wiadomość lub którym opatrzona jest strona www. Nie dajmy się zwieść podobieństwu graficznemu witryny – fałszerze nauczyli się doskonale podrabiać strony internetowe. Zwracajmy uwagę na drobne szczegóły, takie jak błędy literowe, drobne zmiany w kolorystyce, logo, detalach. Oszustom takie wpadki się zdarzają, bo zazwyczaj najtańszym kosztem podszywają się pod strony kosztujące wiele set tysięcy złotych.

Rada druga: wybierajmy wyłącznie łącza szyfrowane protokołem SSL, zapobiegającym przechwyceniu danych. Taką witrynę można poznać po tym, że przed adresem strony, zamiast wywołania „http:” pojawia się formuła „https:”. To podstawowa i zwykle najskuteczniejsza metoda ochrony przesyłanych przez nas informacji.

Wreszcie rada trzecia: podawajmy tylko te dane, które są niezbędne do zawarcia transakcji. Owszem, odmowa udostępnienia informacji może grozić niezrealizowaniem usługi, ale czasem warto oszacować zagrożenie i samodzielnie zdecydować o podjęciu (lub nie) ryzyka.

Na koniec parę słów pocieszenia. Informatyka to tylko narzędzie, samo w sobie bezpieczne, jeśli tylko człowiek świadomie z niego korzysta. Dlatego w podróży większym zagrożeniem niż crakerzy mogą się okazać nasza naiwność i roztargnienie. A bezpieczeństwo informacji zależy nie tyle od wymyślnych zabezpieczeń, ile od naszego zdrowego rozsądku.